Sequential Attack with Intensity Modulation on the Differential-Phase-Shift Quantum Key Distribution Protocol

Toyohiro Tsurumaru

Mitsubishi Electric Corporation,
Information Technology R&D Center
5-1-1 Ofuna, Kamakura-shi,
Kanagawa, 247-8501, Japan

In this paper, we discuss the security of the differential-phase-shift quantum key distribution (DPSQKD) protocol by introducing an improved version of the so-called sequential attack, which was originally discussed by Waks et al.[5]. Our attack differs from the original form of the sequential attack in that the attacker Eve modulates not only the phases but also the amplitude in the superposition of the single-photon states which she sends to the receiver. Concentrating especially on the "discretized gaussian" intensity modulation, we show that our attack is more effective than the individual attack, which had been the best attack up to present. As a result of this, the recent experiment with communication distance of 100km reported by Diamanti et al.[3] turns out to be insecure. Moreover it can be shown that in a practical experimental setup which is commonly used today, the communication distance achievable by the DPSQKD protocol is less than 95km.

I. INTRODUCTION

The differential-phase-shift quantum key distribution (DPSQKD) protocol[4] is a promising protocol for quantum key distribution (QKD) featuring the tolerance against photon number splitting attacks. However, its security has only been investigated so far against limited types of attacks; The most effective attack up to present had been a particular type of individual attacks investigated by Waks et al. [5], in which Eve acts on *photons* individually rather than on *signals*. Several long-distance experiments claiming security along its line have been reported (see, e.g.,[3] and references therein). Another important class of attacks is a variant of intercept-resend attacks called *sequential attacks* which was also discussed originally by Waks et al.[5] and later improved by Curty et al.[2]. However, they still remain less effective than the individual type for most probable applications.

We will here present a further improvement on the sequential attack in which the attacker Eve modulates not only the phases but also the amplitude in the superposition of the single-photon states which she sends to the receiver. In this paper, with a slight abuse of terminology, we call such differentiations in the amplitude an *intensity modulation* and investigate its consequence. Concentrating especially on the "discretized gaussian" intensity modulation, we show that our attack is more effective than the individual attack, which had been the best attack. As a result of this, the recent experiment with communication distance of 100km reported by Diamanti et al.[3] turns out to be insecure. Moreover it can be shown that in a practical experimental setup which is commonly used today, the communication distance achievable by the DPSQKD protocol is less than 95km.

In what follows, we shall consider a conservative definition of security, i.e., we assume that Eve can control some flaws in Alice's and Bob's devices (e.g., the detection efficiency and the dark count probability of the detectors), together with the losses in the channel, and she exploits them to obtain maximal information about the shared key.

II. DPSQKD PROTOCOL

The DPSQKD protocol proceeds as follows[4, 5].

1. Alice generates a random bit string $x = (x_0, \ldots, x_N)$, $x_i \in \{0, 1\}$ and sends to Bob the coherent light pulses with phase $\phi_i = \pi x_i + \phi$ and intensity α, where $\phi, \alpha \in \mathbb{R}$, $\alpha > 0$. That is, Alice generates the following $|\Psi\rangle$ and sends to Bob:

$$|\Psi\rangle = |\alpha e^{i\phi_0}\rangle \otimes \cdots \otimes |\alpha e^{i\phi_N}\rangle.$$

   Intensity α is related to the average photon number $\bar{n}$ per pulse as $\bar{n} = |\alpha|^2$.

2. Using a Mach-Zehnder interferometer (Fig.1), Bob measures the phase difference $z_i = x_i + x_{i-1}$ of each adjacent pair of pulses[6]. The outcome of the measurement is recorded as the sifted key $b = (b_1, \ldots, b_l)$, $b_a = x_{i_a} + x_{i_a-1}$, where $i_1, \ldots, i_l$ are the times when photons are detected.

3. Communicating on an authenticated classical channel, Alice and Bob perform key reconciliation and the generalized privacy amplification[1, 5] to calculate the secret key.

We denote by T the transmission of the communication channel including the loss in fiber and Bob's interferometer, and the quantum efficiency of Bob's detector. We also denote by d the dark count of Bob's detector. Then the signal and detection rate p_{click} at Bob's side is given by

$$p_{\text{click}} = T\bar{n} + d. \qquad (1)$$

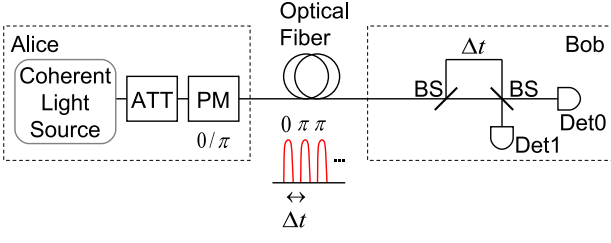Thus in the second step above, the average length l of the sifted key is $l = Np_{\text{click}}$.

FIG. 1: Basic experimental setup of a DPSQKD system. Here PM denotes a phase modulator, and BS a 50:50 beamsplitter. Δt represents the time difference between two consecutive pulses. Photon detectors Det0 and Det1 output the phase differece $z_i = 0$ and 1 respectively.

III. SEQUENTIAL ATTACK WITH INTENSITY MODULATION

In this section, we first define our attack and then calculate several probabilities that are necessary for later analyses, i.e., the error rate which Bob detects as a result of the attack and the success probability of Eve's attack. The necessary conditions for Eve to carry out the attack are also derived in terms of experimental parameters, such as the average photon number $\bar{n}$ and the transmission T.

A. Description of Attack

The basic scheme of our sequential attack is the same as the previous versions given in Ref.[5]. The only difference is that the state Ψ which Eve sends is a superposition of single-photon states with different amplitudes (see Fig.2). The precise definition of our attack is as follows:

1. Using unambiguous state discrimination (USD, see Ref.[2]) measurement, Eve measures the phase x_i of all but small portion of the pulses that Alice sent and records the outcome.

   Here the small portion means a pulse sequence of length ϵN with $\epsilon = (1-r)p_{\text{click}}/\bar{n}$. The ratio $r \in \mathbb{R}$, $0 < r \leq 1$ is a parameter to be specified later.

2. For $rp_{\text{click}}N$ sequential detection events of length k or larger, Eve does as follows:

   If the detected phases were, say, $x_a, \ldots, x_{a+k-1}$, she generates state $|\Phi\rangle$ defined as

   $$|\Phi\rangle := \sum_{i=a-M}^{a+k+M} (-1)^{y_i} A_i a_i^\dagger |0\rangle, \qquad (2)$$

   and sends it to Bob. Here parameter $M \in \mathbb{N}$ is a sufficiently larege number, and y_i are set as $y_i = x_i$ for $a \leq i \leq a+k-1$, and other $y_i \in \{0,1\}$'s are randomly chosen values. The creation operator $a_i^\dagger$ denotes a single photon pulse incident to Bob for time interval i.

3. Eve sends ϵN pulses which she kept intact in the first step, and sends them to Alice.

In what follows, we assume that transmission T and $p_{\text{click}}/\bar{n}$ are small enough (e.g., with the communication distance being sufficiently large) so that ϵ can be neglected.
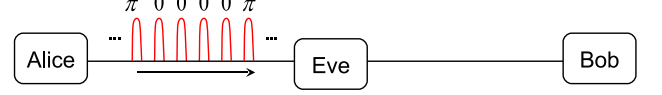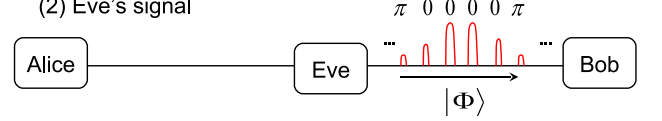

FIG. 2: Graphical image of our sequential attack. (1)Alice emits coherent light pulses with an equal intensity, and Eve detects them. (2)When sequential detection events are found, Eve sends out single-photon state $|\Phi\rangle$ of Eqn.(2), which is a superposition of single-photon states having the same phases as Alice's original signal but with different amplitudes.

B. Probability of Sequential Detection

The USD measurement performed in the first step succeeds for each pulse with probability

$$p_{\text{USD}}(\bar{n}) = 1 - \exp(-2\bar{n}),$$

where $\bar{n} = |\alpha|^2$ is the average number of photon per pulse[2]. It can easily be shown that when Eve repeats it for a sufficiently long sequence of pulses, a sequential detection with length k or larger occurs with probability

$$p_{\text{seq}}(k, \bar{n}) = (1 - p_{\text{USD}}(\bar{n})) (p_{\text{USD}}(\bar{n}))^k. \qquad (3)$$

In other words, as a result of USD measurements on N pulses, Eve finds on average $Np_{\text{seq}}(k, \bar{n})$ events of sequential detections of at least length k. Hence $rp_{\text{click}} \leq p_{\text{seq}}(k, \bar{n})$ is necessary in order for Eve to carry out her attack.

C. Error Rate Due to Φ

Every state $|\Phi\rangle$ sent by Eve in the second step will always yield one detection event in Bob's detector in either of time i. In other words, Bob's overall detection probability of $|\Phi\rangle$ is strictly one. However, the detection can generally occur in a wrong detector causing the bit flip in the sifted key, or it may click in time i where Eve does not know the corresponding phase shift, in which case she fails to steal the sifted key bit.

To evaluate these effects we will below obtain, in terms of the amplitude A_i, the formulae for the error rate $E(k)$ caused by each $|\Phi\rangle$, and the probability $D(k)$ that Eve ends up reading the sifted key bit using $|\Phi\rangle$. In what follows, we suppose that N is sufficiently large and A_i converges to zero fast enough for $i \to \pm\infty$, so that parameter M introduced in the second step of our attack can be regarded as infinite .

Suppose that Eve has succeeded in determining k subsequent phases $x_a, \ldots, x_{a+k-1}$ in the first step and knows the corresponding phase differences $z_{a+1}, \ldots, z_{a+k-1}$. Then in the second step, state $|\Phi\rangle$ of Eqn.(2) sent to Bob evolves inside his interferometer as

$$|\Phi\rangle \; \to \; \frac{1}{2} \sum_{i=-\infty}^{\infty} \left[(-1)^{y_i} A_i + (-1)^{y_{i-1}} A_{i-1} \right] d_{0i}^\dagger |0\rangle \quad (4)$$
$$+ \frac{1}{2} \sum_{i=-\infty}^{\infty} \left[-(-1)^{y_i} A_i + (-1)^{y_{i-1}} A_{i-1} \right] d_{1i}^\dagger |0\rangle,$$

where creation operators $d_{0i}^\dagger$ and $d_{1i}^\dagger$ denotes the single photons incident to the detectors outputting $z_i = 0$ and 1 respectively.

An error in z_i occurs when the spectrum $d_{z_i+1,i}^\dagger |0\rangle$ contained in Eqn.(4) is measured by Bob. Hence Bob detects error with probability

$$E(k) = \frac{1}{4} \sum_{i=-\infty}^{\infty} \left| (-1)^{x_i+y_i} A_i - (-1)^{x_{i-1}+y_{i-1}} A_{i-1} \right|^2 .$$

By summing this over for Eve's random choices of y_i for $i < a$ and $a + k \le i$, we have

$$E(k) \; = \; \frac{1}{4} \sum_{i=a+1}^{a+k-1} |A_i - A_{i-1}|^2 \quad (5)$$
$$+ \frac{1}{4} \left(\sum_{i=-\infty}^{a} + \sum_{i=a+k}^{\infty} \right) \left[|A_i|^2 + |A_{i-1}|^2 \right].$$

On the other hand, Eve ends up knowing Alice and Bob's raw key bit when Bob detects either one of phase differences $z_{a+1}, \ldots, z_{a+k-1}$, which occurs with probability

$$D(k) = \frac{1}{2} \sum_{i=a+1}^{a+k-1} \left[|A_i|^2 + |A_{i-1}|^2 \right] . \quad (6)$$

Note here that we are justified in including error events in $D(k)$ because the corresponding sifted key bit will always match between Eve and Bob due to key reconciliations to be performed later, as long as the detected error rate is smaller than the threshold QBER.

D. Effective Error Rate

Hence in order for Eve to carry out the attack it is sufficient that there exist parameters $1 \le k$ and $0 \le r \le 1$

such that

$$r p_{\text{click}} \; \le \; p_{\text{seq}}(k, \bar{n}), \quad (7)$$
$$r E(k) \; \le \; e_{\text{exp}}, \quad (8)$$

where e_{exp} is the QBER in the absence of Bob. Inequality (7) means that Eve has an enough number of sequential events, and Inequality (8) is to guarantee that the error rate is small enough so that the presence of Eve will not be noticed by Bob. And as a result of the attack, Eve steals $r D(k) N p_{\text{click}}$ bits out of an sifted key of length $N p_{\text{click}}$ bits on average while the error rate measured by Bob is $r E(k)$.

Since key reconciliation and the generalized privacy amplification are used in the secret key generation of the DPSQKD [1, 5], the key generation rate R is bounded from above as

$$R \; \le \; p_{\text{click}} \left(I(A;B) - I(A;E) \right)$$
$$= \; p_{\text{click}} \left(1 - H_2(e_{\text{exp}}) - r D(k) \right),$$

where $I(A;B)$ and $I(A;E)$ are the mutual informations between Alice and Bob, and between Alice and Eve, respectively. Clearly, $I(A;B)$ equals $1 - H_2(e_{\text{exp}})$ with $H_2(x)$ being the binary entropy function $H_2(x) := -x \log_2 x - (1-x) \log_2(1-x)$, and $I(A;E)$ is given by $r D(k)$ in our sequential attack.

Thus if Eve is not interested in obtaining as many sifted key bits as possible, but rather she is only willing to invalidate the key distribution between Alice and Bob, the best strategy for her is to minimize the error rate $r E(k)$ by suppressing the ratio r. That is, when Inequalities (7) and (8) are satisfied for $r = 1$ and a certain value of k, the error rate $r E(k)$ measured by Bob can be further reduced by taking r such that

$$1 - H_2\left(r E(k)\right) - r D(k) = 0. \quad (9)$$

In what follows, we will call such minimum value of $r E(k)$ the effective error rate and denote it by $E_{\text{eff}}(k)$.

IV. GAUSSIAN INTENSITY MODULATION

In the original form of sequential attacks as introduced by Waks et al.[5], the amplitude A_is were

$$A_i = \begin{cases} 1/\sqrt{k} & \text{for } a \le i \le a+k-1, \\ 0 & \text{otherwise,} \end{cases}$$

for which the error and detection rates were

$$E(k) = 1/2k, \text{ and } D(k) = (k-1)/k. \quad (10)$$

In this section we demonstrate how these can be improved by selecting an appropriate wave form for A_i.

One can generally seek for the best attack strategy, i.e., the best pattern of A_i with the smallest $E(k)$ possible for each value of k while maintaining the enough

ratio $D(k)$ of bits accessible to Eve, as long as ks are sufficiently small. Indeed it is not difficult at all to find out the best A_i, e.g., by doing numerical simulations, but in this paper, as the first trial, we will concentrate on the following (discretized) gaussian pattern:

$$A_i = C \exp\left[-\frac{(i-c)^2}{4\sigma^2}\right]. \qquad (11)$$

The constant C appearing on the right hand side normalizes $|\Phi\rangle$ as $\sum_n |A_n|^2 = 1$, c denotes the time offset, and σ is the standard deviation to be adjusted later. For the present we will set c at the center of Eve's detected signals, i.e., when Eve has detected phases $x_a, \cdots, x_{a+k-1}$, we set $c = a + (k-1)/2$.

A. First-Order Approximation of $E(k)$ and $D(k)$

In order to have a rough idea as to how effective the gaussian intensity modulation in Eqn.(11) is, we first investigate it in the continuous limit of $k, \sigma \to \infty$, where $E(k)$ and $D(k)$ given in Eqn.(5) and (6) can be explicitly calculated. In this limit $C \to (\sqrt{2\pi}\sigma)^{-1/2}$ and we have

$$
\begin{aligned}
E(k) &= \frac{|C|^2}{4} \sum_{i=-\infty}^{\infty} |A_i - A_{i-1}|^2 \\
&\quad + \frac{|C|^2}{2}\left(\sum_{i=-\infty}^{a} + \sum_{i=a+k}^{\infty}\right) A_i A_{i-1} \\
&= \frac{|C|^2}{2} \sum_{i=-\infty}^{\infty}\left(e^{\frac{-(i-c)^2}{2\sigma^2}} - e^{-\frac{(i-c-1/2)^2}{2\sigma^2} - \frac{1}{8\sigma^2}}\right) \\
&\quad - |C|^2 e^{-\frac{1}{8\sigma^2}} \sum_{i=a+k}^{\infty} e^{-\frac{(i-c-1/2)^2}{2\sigma^2}} \\
&\simeq \frac{1}{2}\left(1 - e^{-1/8\sigma^2}\right) + \frac{e^{-1/8\sigma^2}}{\sqrt{2\pi}}\int_{k/2\sigma}^{\infty} dx\ e^{-x^2/2} \\
&\simeq \frac{1}{16\sigma^2} + 1 - \operatorname{erf}\left(\frac{k}{2\sqrt{2}\sigma}\right)
\end{aligned}
$$

with $\operatorname{erf}(\cdot)$ being the error function

$$\operatorname{erf}(x) := \frac{2}{\sqrt{\pi}}\int_0^x dt\ e^{-t^2}.$$

Thus by choosing $k = 4\sigma$ for example, we have $E(k) \simeq 1/k^2 + 0.0228$, which is far smaller than Eqn.(10). Similarly, the detection rate can be calculated as

$$D(k) \simeq \frac{1}{\sqrt{2\pi}}\int_{-k/2\sigma}^{k/2\sigma} dx\ e^{-x^2/2} = \operatorname{erf}\left(\frac{k}{2\sqrt{2}\sigma}\right).$$

B. Corrections Due to Discretization

In reality, we must take into account the corrections due to dicretization. Adjusting values of σ, we numerically calculated for each value of k the smallest of error

rate $E(k)$ as shown in Table I. These values agree with the above first-order approximation within 10% for $k \geq 8$.

k	σ	$E(k)$	$D(k)$	$E_{\text{eff}}(k)$
4	0.871	0.105	0.881	0.0614
5	1.03	0.0748	0.930	0.0495
6	1.18	0.0562	0.954	0.0405
7	1.34	0.0438	0.968	0.0335
8	1.49	0.0353	0.977	0.0282
9	1.63	0.0290	0.982	0.0239
10	1.78	0.0243	0.987	0.0206

TABLE I: The smallest error rate $E(k)$ caused by $|\Phi\rangle$ with the gaussian intensity modulation given in Eqn.(11). These minimums are obtained by adjusting the standard deviation σ for each value of k. Here k denotes the length of Eve's sequential detection, $D(k)$ the corresponding detection rate, and $E_{\text{eff}}(k)$ the effective error rate measured by Bob.

V. COMPARISONS WITH EXPERIMENTS

In this section, we discuss how our attack limits communication distances of the DPSQKD experiments. The main purpose here is to show that in many of practical experimental setups, our attack works more effectively than the individual attack introduce by Waks et al.[5], hence reevaluating the security of several experiments reported up to now.

We will first show that the experiment with a communication distance of 100km reported by Diamanti et al.[3] is in fact insecure. Then we will also show that for a set of parameter values which are commonly used in today's QKD experiments and security analysis, e.g. in Ref.[3, 5], the DPSQKD cannot be secure for distances larger than 95km no matter how one adjusts the average photon number $\bar{n}$.

A. 100km Experiment by Diamanti et al.

Diamanti et al.[3] performed a DPSQKD experiment with communication distance of 100km using the following set of parameters:

- Average photon number $\bar{n} = 0.2$,

- Optical fiber of 100km = loss of 20dB,

- Bob's Mach-Zehnder interferometer = loss of 2dB,

- Efficiency of Bob's detector = 4×10^{-3},

- Bob's dark count probability $d = 3.5 \times 10^{-8}$,

from which Bob's signal and dark count rate p_{click} of Eqn.(1) can be calculated as

$$p_{\text{click}} = 5.12 \times 10^{-6}$$

and the QBER they measured was

$$e_{\text{exp}} = 3.4\%.$$

With these values, however, Eve can mount our sequential attack with $k = 9$ and invalidate the secret key distribution. The conditions (7) and (8) for $k = 9$ are satisfied since $p_{\text{click}} < p_{\text{seq}}(k = 9, \bar{n} = 0.2) = 3.08 \times 10^{-5}$ as can be found from Eqn.(3), and $E_{\text{eff}}(9) = 2.39\% < e_{\text{exp}}$ from Table I.

B. Limitations on the Communication Distance for a Practical Setup

Next we compare our result with a more general set of experimental parameters given in Refs.[3] and [5].

The signal and the dark count detection probability p_{click} is as given in (1), where the transmission T typically takes the form

$$T = \eta_{\text{int}} \eta_{\text{det}} 10^{-\alpha_{\text{fiber}} L/10}.$$

Here $\alpha_{\text{fiber}} = 0.2$dB/km is the fiber attenuation, L the fiber length, $\eta_{\text{int}} = 2$dB the loss in Bob's Mach-Zehnder interferometer[3], and $\eta_{\text{det}} = 0.1$ the quantum efficiency of Bob's detector[5].

On the other hand, the error rate in the absence of Eve is given by

$$e_{\text{exp}} = \frac{\mu p_{\text{click}} + d/2}{p_{\text{click}}}, \qquad (12)$$

where μ is the baseline error rate of the system due to imperfections in the state preparation, channel induced noise, and imperfect detection apparatus [5]. The typical values for μ and the dark count d are $\mu = 0.01$ and $d = 10^{-5}$[5].

Now let the communication distance $L = 95$km, or $T = 10^{-3.1}$ (loss of 31dB). Then it can be shown that key distribution is shown to be impossible for any value of $\bar{n}$ as follows; For $\bar{n} \leq 0.14$ and $0.36 \leq \bar{n}$, the gain formula R_{ind} based on individual attack[5] yields negative values:

$$R_{\text{ind}} = -p_{\text{click}} \left[(1 - 2\bar{n}) \log_2 P_{C_0} + H_2(e_{\text{exp}}) \right],$$
$$P_{C_0} \leq 1 - e_{\text{exp}}^2 - \frac{(1 - 6e_{\text{exp}})^2}{2}.$$

On the other hand, for $\bar{n} \leq 0.14$ and $0.36 \leq \bar{n}$, Inequalities (7) and (8) are satisfied for values of k given in Table II. For example, Eve can mount the attack for $k = 9$ when $0.30 \leq \bar{n} \leq 0.36$ because in this parameter region, $p_{\text{seq}}(9, \bar{n}) - p_{\text{click}}$ and $e_{\text{exp}}(\bar{n}, T)$ are

both monotonically increasing in $\bar{n}$, and it holds that for $\bar{n} = 0.30$, $p_{\text{seq}}(9, \bar{n} = 0.30) > p_{\text{click}}(T, \bar{n} = 0.30)$ and $e_{\text{exp}}(T, \bar{n} = 0.30) = 0.0302 > E_{\text{eff}}(9) = 0.239$. The effectiveness in other regions can be shown similarly.

$\bar{n}$	Attack Type	k
$0 \sim 0.14$	individual	–
$0.14 \sim 0.19$	sequential	6
$0.19 \sim 0.25$	sequential	7
$0.25 \sim 0.30$	sequential	8
$0.30 \sim 0.36$	sequential	9
$0.36 \sim \infty$	individual	–

TABLE II: The list of suitable attack type for a 95km DP-SQKD experiment depending on parameter regions of the average photon number $\bar{n}$. The corresponding length k of a sequential detection event are also shown in the right column.

VI. CONCLUSION

In this paper, we presented an improved version of sequential attacks with intensity modulation, which works more effectively than the individual attack. Using this attack, we have shown that the recent experiment with communication distance of 100km reported by Diamanti et al.[3] is in fact insecure. We also showed that in a practical experimental setup which is commonly used today, the communication distance achievable by the DPSQKD protocol is less than 95km.

There are several straightforward ways to improve our result. First, although we restricted ourselves in this paper to the discretized gaussian distribution of Eqn.(11), numerically optimizing A_i can yield a better form of state $|\Phi\rangle$ with smaller error rate $E(k)$ while maintaining detection rate $D(k)$, as mentioned at the beginning of Sec.IV. Moreover, by letting $|\Phi\rangle$ be a superposition of states with different photon numbers, we can increase the detection counts caused by each $|\Phi\rangle$ to more than one. For instance, instead of the single-photon state $|\Phi\rangle$ given in Eqn.(2), it is possible that a coherent state

$$|\Phi_{\text{coh}}\rangle = \exp \left(\sum_i (-1)^{y_i} A_i a_i^{\dagger} + \text{h.c.} \right) |0\rangle$$

leads to a more effective attack. Here h.c. stands for hermite conjugate. Note that the norm $\sum_i |A_i|^2$ of A_i corresponds to the average photon number contained in this state and need not be normalized.

[1] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized Privacy Amplification," IEEE Trans. IT-41, 1915 (1995).

[2] M. Curty, L.-L. Zhang, H.-K. Lo, and N. Lütkenhaus, "Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states," arxiv.org, quant-ph/0609094, (2006).

[3] E. Diamanti, H. Takesue, C. Langlock, M. M. Fejer, and Y. Yamamoto, "100km secure differential phase shift quantum key distribution with low jitter up-conversion detectors," arXiv.org, quant-ph/0608110 (2006).

[4] K. Inoue, E. Waks, and Y. Yamamoto, "Differential Phase Shift Quantum Key Distribution," Phys.Rev.Lett.,89, 037902 (2002).

[5] E. Waks, H. Takesue, and Y. Yamamoto, "Security of differential-phase-shift quantum key distribution against individual attacks," Phys. Rev. A, 73, 012344 (2006).

[6] Throughout this paper, summations over x_i, z_i, b_i are always in modulo 2.